IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TENNESSEE

STATE OF TENNESSEE

COUNTY OF SHELBY

Case No. 23-SW-491

ATTACHMENT C

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, **Keyotta Sanford**, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the FBI assigned to the Memphis Division and have been a Special Agent since January 2019. I am currently assigned to the Child Exploitation & Human Trafficking Task Force, investigating matters involving the sexual exploitation of children, human trafficking, and child sexual abuse material (CSAM). I have participated in various trainings and investigations involving online and computer related offenses and have executed numerous search warrants, including those involving searches and seizure of computers, digital media and electronically stored information.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination and analysis of data for electronic devices described in **Attachment A**, which are currently in law enforcement possession, for contraband, evidence, fruits and instrumentalities of violations of 18 U.S.C. § 2251(a) (production of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), which items are more specifically described in **Attachment B**.

3. The statements in this affidavit are based in part on information provided by other

KS
12/1/2023

sworn law enforcement officers participating in this investigation, through observations and conversations of your affiant personally, and through other sources specifically named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence in violation of 18 U.S.C. § 2251(a) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) will be found on the devices described in **Attachment A**, and electronically stored information will consist of or be contained in the items listed in **Attachment B**, both of which are incorporated by reference as if fully set forth herein.

STATUTORY AUTHORITY

4. 18 U.S.C. §§ 2251(a) makes it a federal offense for anyone to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in sexually explicit conduct as defined in 18 U.S.C. §§ 2256, for the purpose of producing a visual depiction of such conduct, or attempts to do so.

5. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

KS
12/1/2023

DEFINITIONS

6. The following definitions apply to this affidavit and **Attachment B**:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal

KS
12/1/2023

and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to

KS
12/1/2023

the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

k. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

l. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

CHARACTERISTICS OF INDIVIDUALS WHO PRODUCE AND POSSESS CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, there are certain characteristics that are

KS
12/1/2023

prevalent among individuals who are involved in the production and receipt of child pornography:

a. The majority of individuals who produce and possess child pornography are persons who have a sexual attraction to children, and may engage in the sexual abuse of children or exchange and collect child pornography and child erotica to receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

b. Individuals who produce and possess child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videos, drawings or other visual media. Not only do these individuals oftentimes use these materials for their own sexual arousal and gratification, but they also may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. The majority of individuals who collect, receive and produce child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. Individuals who collect and produce child pornography often correspond with and/or meet others to share information and materials and often maintain lists of names, usernames, addresses, emails, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography and child sexual abuse.

d. Persons committing these criminal acts, more likely than not, almost always possess and maintain their hard copy and/or digital medium collections of child pornographic and child erotica material in a secure and private environment. Due to the psychological support their collections provide, such individuals find comfort and justification for their illicit behavior and desires and rarely destroy such materials. As such, these collections are often maintained for several years and are

KS
12/1/2023

kept close by, usually in a location that is mobile and/or easily accessible to the individual.

e. In some cases, people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers of digital devices. Traces of such activity can often be found on computers or digital devices for months or even years after any downloaded files have been deleted.

f. Individuals that produce and possess child pornography frequently prefer not to be without their child pornography for any prolonged time period, and more likely than not may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. This behavior has been documented by law enforcement officers involved in child exploitation and pornography investigations worldwide.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

8. The devices are currently in the possession of the Federal Bureau of Investigation Memphis Division and were obtained by the Tipton County Sheriff's pursuant State of Tennessee search warrant. Your affiant seeks this additional warrant out of an abundance of caution to be certain that the seizure and examination of the devices will comply with the Fourth Amendment and other applicable laws.

9. On November 20, 2023, the FBI Memphis Child Exploitation and Human Trafficking Task Force (CEHTTF) received a tip from the Tipton County Sheriff's Office (TCSO) regarding allegations that a registered sex offender had taken nude images of a13-year-old relative.

10. According to the TCSO, on or around 11/19/2023, Deputies responded to complaint in Covington, TN involving the sexual assault of a 13-year-old female by a relative at their residence. Deputies identified the victim's relative as Jarrod Sanford (Sanford), who was a registered sex offender. While on scene, the minor victim told the Deputies that Sanford had

IKS
12/1/2023

sexually assaulted her the day prior. The victim also provided Deputies with a cell phone that she advised belonged to Sanford, who had given it to her when police arrived at the residence. Sanford told her that he did not want the phone to be provided to law enforcement. Additionally, the minor told Deputies that she believed Sanford had taken nude images of her utilizing the phone.

11. On November 20, 2023, a child forensic interview was conducted with the minor victim. During her interview, the victim disclosed she had been sexually assaulted by Sanford on more than one occasion. The minor confirmed she told police that Sanford had taken nude images of her and recalled an incident in which she could hear a noise similar to that of a cell phone taking a picture and recording a video. The minor further advised that this occurred while she was being sexually assaulted by Sanford and while he was holding her head down.

12. On November 20, 2023, a State of Tennessee search warrant was issued for a black and silver in color Android cell phone, which was provided to TCSO Deputies and identified as being used by Sanford to take nude images of the minor victim.

13. On November 20, 2023, your affiant confirmed with the U.S. Attorney's Office and the U.S. Probation Office that Jarrod Steven Sanford was on Federal Probation for life due to sexual offenses and was not allowed to have any media devices that were not monitored by the U.S. Probation Office.

14. On November 21, 2023, a federal search warrant was executed on the Android cell phone, which was identified as being utilized by Sanford to take nude images of the minor victim. Pursuant a forensic examination of the device, images consistent with CSAM were observed. In particular, your affiant observed what appeared to be images an unknown female performing oral sex on an unknown male. Based on a comparison of a known image of the minor victim, it was believed the unknown female and the minor victim were one and the same. Your affiant also

KS
12/1/2023

observed an image of what appeared to be an individual holding a cell phone, with a picture of nude erect penis visible on the screen.

15. On November 22, 2023, investigators interviewed an adult relative of the minor victim. During the interview, the minor victim was positively identified as the unknown female performing oral sex on an unknown male.

16. On November 22, 2023, a federal arrest warrant was issued for Sanford, who was later detained that same day by the U.S. Marshals. He was arrested in his truck, and in the center console of the truck the deputy marshals found a black in color Android cell phone, with the word "BLU" displayed on the back. They seized the phone and identified it as belonging to Sanford.

17. On November 27, 2023, the minor victim was forensically interviewed by a FBI Child Adolescent Forensic Interviewer. During the interview, the minor victim was shown images which were obtained from a forensic extraction of an Android cell phone, identified as belonging to Sanford. The minor victim positively identified herself within the images and advised Sanford had forced her to perform oral sex on him, in the living room of his residence. The minor victim also disclosed being sexually assaulted by Sanford on numerous occasions, starting around when she was approximately 12 years of age. The sexual assaults occurred within Sanford's residence in Covington, Tennessee.

18. On November 28, 2023, a State of Tennessee search warrant was issued to search the residence of Sanford, located at 2154 Bringle Rd, Covington, Tennessee 38019, which was identified by the minor victim as the place in which she was sexually assaulted by Sanford. TCSO Deputies identified and seized multiple additional electronic devices, some of which were believed to have been unauthorized and against the terms of Sanford's probation. Based on the evidence already found on the devices, including the photo of a yet-unidentified cell phone displaying a

KS
12/1/2023

picture of a nude erect penis, there is probable cause to believe that these additional devices were used in the commission of the alleged crimes.

19. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. § 2251(a) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) have been committed, and evidence, instrumentalities and fruits of those violations are located on the devices further described in **Attachments A and B** of this affidavit.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge and experience, cellular phones can also be considered portable data storage devices which contain several data storage features contained in one device. I know that deleted photos or deleted text message can likely be retrieved from cell phones and valuable information cannot be obtained through cell phone records maintained by the cell phone provider. There are various applications which are intended to be installed on Smart phones. These third party applications are intended to communicate with the cell network, Internet, or the phone's communication features. I know these applications can be used for monetary transactions, email, short message services (SMS), Multi-Media Services (MMS) and for placing Internet-based phone calls. I know based on my training and experience that data found in the databases of installed applications are relevant to criminal investigations.

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Subject devices may still be stored there, for at least the following reasons:

IKS
12/1/2023

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -that is, in space on the storage medium that is not currently being used by an active file -for long periods of time before they are overwritten. In addition, a computer's operating system also may keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

KS
12/1/2023

23. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can 15 record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

KS
12/1/2023

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to participate or promote sex trafficking by force, fraud, or coercion, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain the following: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offenses and identity of the perpetrator(s).

24. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not

KS
12/1/2023

limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution*. Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the court to authorize execution of the warrant at any time in the day or night.

JURISDICTION

26. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

27. I believe that based upon the totality of facts and circumstances described above, probable cause exists to search the devices described above for evidence and instrumentalities of and concerning violations of 18 U.S.C. § 2251(a) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). In consideration of the foregoing, your affiant respectfully requests that this Court issue a search warrant authorizing the examination, analysis and review of the devices more specifically described in **Attachment A**, authorizing the search and seizure of the items described in **Attachment B**, incorporated herein.

AND FURTHER, AFFIANT SAITH NOT.

Keyotta Sanford - AFFIANT
Special Agent,
Federal Bureau of Investigation.

KS
12/1/2023

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 1st day of December, 2023.

HON. ANNIE T. CHRISTOFF
United States Magistrate Judge